Experiences with Paste-Monitoring

OWASP BeNeLux Day 2016

CIRCL
Computer Incident
Response Center
Luxembourg

Michael Hamm - *TLP:WHITE*

info@circl.lu

17.-18. March 2016;
Esch-Belval, Luxembourg

CIRCL
Computer Incident
Response Center
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
- CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg.

CERT point of view

- Help
  - Acts like a fire brigade
  - Take all reported incidents serious
  - Help: triage, analysis and response
  - Help: technical investigation
  - Reliable and trusted point of contact
  - No duty to report to the police
  - Victim's duty to file a complaint
- Prevent incidents
  - Early detection
  - Proactive security

CERT services/tools

- Malware Information Sharing Platform - MISP
  - https://www.circl.lu/services/misp-malware-information-sharing-platform/
- URL Abuse Testing
  - https://www.circl.lu/services/urlabuse/
- Dynamic Malware Analysis Platform - DMA
  - https://www.circl.lu/services/dynamic-malware-analysis/
- Paste Monitoring & Analysis of Information Leaks Framework - AIL
  - https://github.com/CIRCL/pystemon
  - https://github.com/CIRCL/AIL-framework

Paste Monitoring

- Example: `http://pastebin.com/`
  - Store text online, easy sharing
  - Used by programmers
  - Source code & configuration information
- Abused by attackers to store:
  - Exploit code
  - Results of running malicious code
  - D0x
  - List of open proxys
  - Anouncements OP...
  - –>Examples: #OpAlQeeq #OpIsrael #OpSaveGaza

Paste Monitoring: General examples

text 1.70 KB raw download clone embed report print

```
卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐
impact-mailorder.de hacked by National Sozialistische Hacker Crew
卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐
Seid gegrüsst Zeckenpack!!
Da ihr hinterlistigen Abschaum-Gestalten immer wieder Angriffe auf unsere Shops und unsere Seiten unternehmt und
anschliessend die Daten online stellt, dachten wir uns, wir drehen den Spiess mal um!

Wir haben nun Namen, Adressen und Telefonnummern, allen die jemals in diesem Shop bestellt haben.
Wir werden davon 40'000 sofort veröffentlichen.
Die restlichen werden wir noch behalten.
Mit jedem Hackerangriff von linksgerichteten Ursprungs auf nationale Adressen werden weitere 10'000 Daten
veröffentlicht!

Es grüsst der Nationale Widerstand, alle Kameraden!

Und euch Zeckenpack sei gesagt: WE ARE WATCHING YOU!
卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐卐
Die ersten 40'000 Daten
Formation:
Name:Vorname:Nachname:Strasse:Ort:Land:Nummer:Email
Download Links:
http://krautchan.net/files/1421870955001.zip
https://neuschwabenland.org/m/src/1421870955001.zip
http://www67.zippyshare.com/v/P9hVIhBK/file.html
```

Paste Monitoring: General examples

#OpISIS- Expose & Destroy By Anonymous RedCult - Pastebin.com
pastebin.com/d8ND4rvV

Feb 8, 2015 **... We are Anonymous**, We are Legion, We do not forgive, We do not forget, Expect us. -Now, Some of ISIS's Twitter accounts, Sites, Emails that ...

OPisis **WE ARE ANONYMOUS** - Pastebin.com
pastebin.com/PkM9A6iv

OPisis **WE ARE ANONYMOUS**. a guest Jan 3rd, 2016 60 Never. rawdownload cloneembedreportprint text 2.36 KB. These are isis accounts and supporter ...

Greetings citizens of the world. **We are anonymous**. The Flint water **...**
pastebin.com/1VHdK8MM

Jan 29, 2016 **... We are anonymous**. The Flint water crisis has drawn the attention of anonymous. Anonymous would first like to pay respect to the victims of this ...

We are Anonymous #opJapane - Pastebin.com
pastebin.com/59RVYN9f

12 hours ago **... We are Anonymous**. #opJapane. RAW Paste Data. **We are Anonymous** # opJapane. create new paste / api / trends / syntax languages / faq ...

Hundreds of ISIS Accounts! - Pastebin.com
pastebin.com/N9rPZ3Ar

Nov 15, 2015 **... We Are Anonymous**,. We Do Not Forgive,. We Do Not Forget,. Expect us! We are the collective today we bring you a mass amount of isis twitter ...

[APT Sources] **We are #Anonymous** - Pastebin.com
pastebin.com/8EF3NyhM

Aug 12, 2015 **...** Kancolle Summer Event 2015: Limited Time Area "Counter Attack! Second SN Operation" will start soon! The operation will last around 20 days ...

Paste Monitoring

- Results of running malicious code
  - Results of port- and vulnerability scans
  - Lists with vulnerable sites
  - Lists with compromised sites
  - Database dumps
  - Credit Card details
  - Leaked 3rd party credentials

Paste Monitoring: General examples

```
[+] Nmap scan report for l[redacted]p.de (85[redacted].227.180)
Host is up (0.016s latency).
Not shown: 64983 closed ports

PORT      STATE    SERVICE
21/tcp    open     ftp
80/tcp    open     http
111/tcp   open     rpcbind
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
3306/tcp  open     mysql
4224/tcp  open     xtell
5666/tcp  filtered nrpe
8193/tcp  open     sophos
25561/tcp open     unknown
25565/tcp open     minecraft
25665/tcp filtered unknown
33517/tcp open     unknown
36123/tcp open     unknown
44121/tcp open     unknown
47084/tcp open     unknown
```

Paste Monitoring

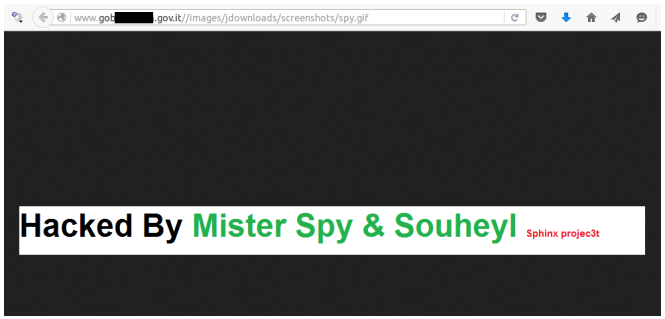
- Statistics
  - Monitoring up to 30 sources
  - Average 1.800.000 pastes/month
  - >100 keywords (constituency)
  - Leads to 5.250 tickets/month
  - Leads to 35 incidents/month
  - Leads to 140 investigation/month
  - Average 7 investigations/day
  - One investgation: 5 minutes - 1 hours
- Challanges
  - Unstructured data

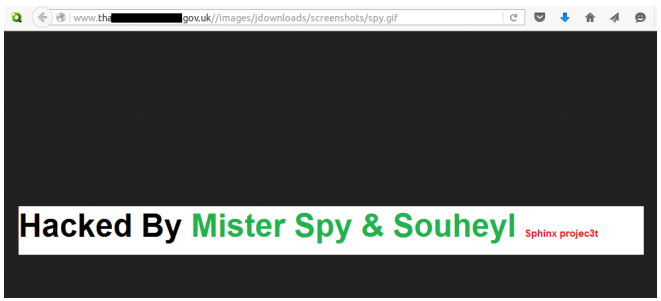
CIRCL #219393 List of URLs

http://www.gasxxxx.com//images/jdownloads/screenshots/spy.gif
http://burytoxxxx.co.uk//images/jdownloads/screenshots/spy.gif
http://sheriasxxxx.coop//images/jdownloads/screenshots/spy.gif
http://www.exxxx.org//images/jdownloads/screenshots/spy.gif
http://www.bexxxx.com//images/jdownloads/screenshots/spy.gif
http://south-xxxx.com//images/jdownloads/screenshots/spy.gif
http://ixxx.org//images/jdownloads/screenshots/spy.gif
http://www.exxxx.com.au//images/jdownloads/screenshots/spy.gif
http://www.alphamxxxxxxxxx.co.za//images/jdownloads/screenshots/spy.gif
http://www.tablemxxxxxxxx.com//images/jdownloads/screenshots/spy.gif
http://www.dubairealdxxxxxxxxx.com//images/jdownloads/screenshots/spy.gif
http://www.world-xxxxx.com//images/jdownloads/screenshots/spy.gif
http://www.nepalmxxxxxxxxx.com//images/jdownloads/screenshots/spy.gif
http://www.proxxx.xxx.gov.ph//images/jdownloads/screenshots/spy.gif
http://www.ajxxx.com//images/jdownloads/screenshots/spy.gif
http://www.fcfmixxxxxx.com//images/jdownloads/screenshots/spy.gif
http://mdxxxx.org//images/jdownloads/screenshots/spy.gif
http://www.lsxxxx.com//images/jdownloads/screenshots/spy.gif
http://pxxxx.com//images/jdownloads/screenshots/spy.gif
http://www.contxxxxx.net//images/jdownloads/screenshots/spy.gif
http://info.farmixxxxxx.fi//images/jdownloads/screenshots/spy.gif
http://www.flxx.be//images/jdownloads/screenshots/spy.gif
http://www.solidxxxx.at//images/jdownloads/screenshots/spy.gif
http://www.xxxx.xtc.br//images/jdownloads/screenshots/spy.gif
http://www.fexxxxx.at//images/jdownloads/screenshots/spy.gif
http://ontarioxxxxxxxxx.ca//images/jdownloads/screenshots/spy.gif

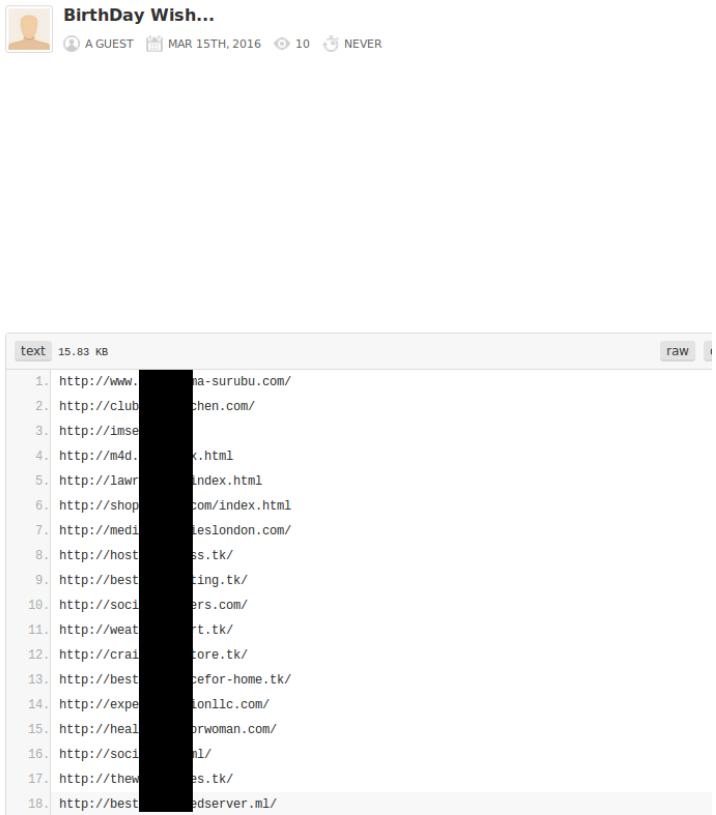
CIRCL #219393 What is behind this URLs?

http://www.pxxxxx.xxx.gov.ph//images/jdownloads/screenshots/spy.gif
http://www.xxxxx.gov.zm//images/jdownloads/screenshots/spy.gif
http://www.xxx.gov.zm//images/jdownloads/screenshots/spy.gif
http://www.xxxxx.gov.zm//images/jdownloads/screenshots/spy.gif
http://www.xxxxxxxxxx.gov.it//images/jdownloads/screenshots/spy.gif
http://www.xxxxxxxxxx.gov.uk//images/jdownloads/screenshots/spy.gif
http://www.goxxxxxxxxxx.gov.it//images/jdownloads/screenshots/spy.gif





CIRCL #223483 What is behind this URLs?



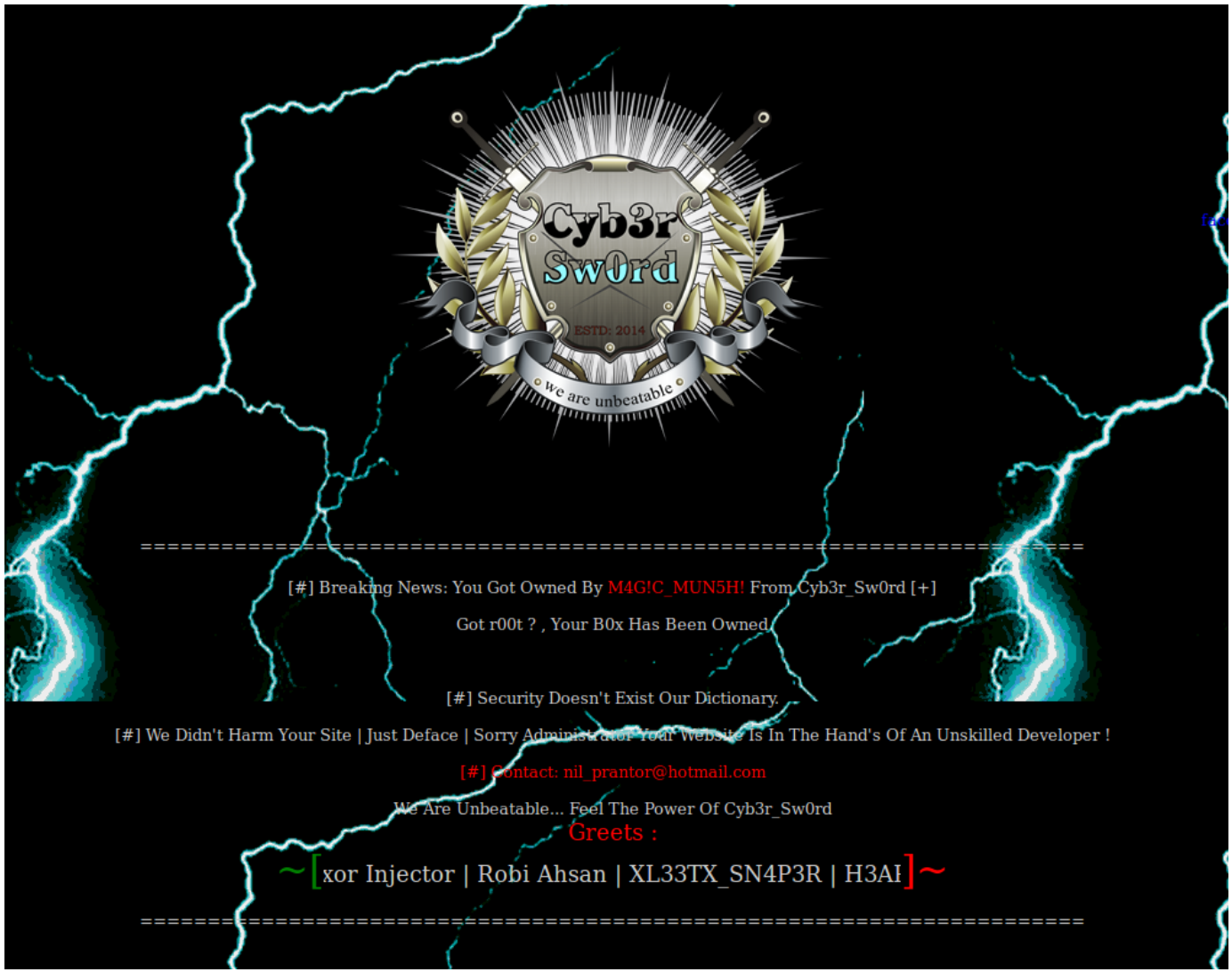
BirthDay Wish...

A GUEST MAR 15TH, 2016 10 NEVER

text 15.83 KB raw

```
1.  http://www.[redacted]ma-surubu.com/
2.  http://club[redacted]chen.com/
3.  http://imse[redacted]
4.  http://m4d.[redacted]x.html
5.  http://lawr[redacted]index.html
6.  http://shop[redacted]com/index.html
7.  http://medi[redacted]leslondon.com/
8.  http://host[redacted]ss.tk/
9.  http://best[redacted]ting.tk/
10. http://soci[redacted]ers.com/
11. http://weat[redacted]rt.tk/
12. http://crai[redacted]tore.tk/
13. http://best[redacted]cefor-home.tk/
14. http://expe[redacted]ionllc.com/
15. http://heal[redacted]orwoman.com/
16. http://soci[redacted]ml/
17. http://thew[redacted]es.tk/
18. http://best[redacted]edserver.ml/
```

CIRCL #223483 Defacements



Results of running malicious code

- How can we help?
  - Report to the website owner (constituency)
  - –>Give advices to them
  - Report to other CERTs
- What we can not do?
  - Contact all website owners outside our constituency

CIRCL #215347 The posting

Target = cpluxxxxxxxxxx.com
zul.xxxxx@ymail.com:5a9ac42d67ab0f139848bb0404355051e0dc6fcd10a22e2ca
ziyanxxxx@yahoo.com:46fe7a6944f6f2bfcebfdef6f06850d94eec1dc02b7722504
xxxxx@teclait.com:092cb6b0a6fb718f20f7704b41173ed52e938432f34a6f389
bscxxxxx@yahoo.com:d93999a44413a63f2dd4e176a349728a23f73aac492a69fcc
yoxxxxx@yahoo.com:e1171a55671a08ec2350902199ba774f82e95f34efe762616
yoogesxxxxx@yahoo.com:451a40fb63d53411f86f4f49b21cc468b058c59a4d41f2fe2
yixxxxxx@upei.ca:614a858c8643cf7e307fd634364f7d6c235f96837c49d0bd4
yinguxxxxx@ou.edu:e85962e3ee35e3f90fb356485c8ebe5b9ec042bac77f1c190
ygxxxxxx@gmail.com:80674b810fc53e53e048f6aacc3c055ddeb349998b9fc5b1a
yemioyxxxxx@yahoo.com:80a0a943d1f509925c7c5552842b4624c2b8effa0d2ec1791
yanninxxxxx@hotmail.com:c18d74cdda28c86615474636d20e2dc5c0b6f2605d570717a
yanghxxxxx@gmail.com:bd4cccf43e5eeee42ec13879f9b0dfd3c5f519658638f3f90
yahya.xxxxx@gmail.com:e61a87f807ec0e2d3f936a7cec7cb5dca8291060ddd212b4b
bendehbia.xxxxxx@hotmail.fr:65324f3ad8e3e85a51740787cf1d1d4bba5c0b84e130e7c60
write2sxxxxxxxxxx@gmail.com:20404051a1d5e96aa0f3a038bd15ce8854b8bbc9b67c2883c
wmsxxxxx@comcast.net:334780689a0ff89ee1034e909bb0bb0bfb4fd732afd7658cf
wincyxxx@hotmail.com:681505cf1cb3907277a081c34c1b72df800d0279d48804e38
jacktxxxxx@yahoo.com:51d94e5885764f3aec7058ba3f28107bcf49c5e79401c3fd6
whitegxxxxxxx@yahoo.com:79918c71701ab71bae7d700d67fd286d21b2f9c3ec513b7e1
whitegxxxxxxx@gmail.com:bc3950cf307a9bc54f103a7ed5275bf724b485c6f1b406bdd

Leaked 3rd party credentials

- How can we help?
  - Report to the ISPs (constituency)
  - –>Advice victims to change this password
  - –>Change it everywhere
  - Report to the targeted website owner
  - Report to other CERTs

  What to avoid to report?
  - Re-postings
  - Old passwords
  - Issues that are already fixed
  - Unknow targeted site
  - Encrypted passwords
  - –>We can give no advices

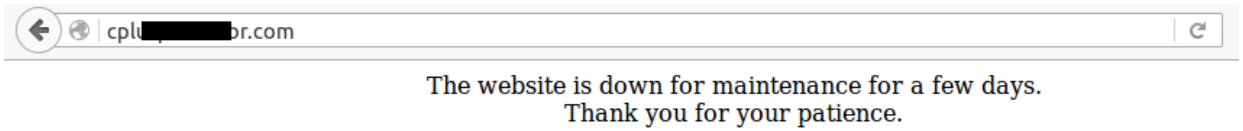
CIRCL #215347 The posting

Target = cpluxxxxxxxxxx.com
zul.xxxxx@ymail.com:5a9ac42d67ab0f139848bb0404355051e0dc6fcd10a22e2ca
ziyanxxxx@yahoo.com:46fe7a6944f6f2bfcebfdef6f06850d94eec1dc02b7722504
xxxxx@teclait.com:092cb6b0a6fb718f20f7704b41173ed52e938432f34a6f389
bscxxxxx@yahoo.com:d93999a44413a63f2dd4e176a349728a23f73aac492a69fcc
yoxxxxx@yahoo.com:e1171a55671a08ec2350902199ba774f82e95f34efe762616
yoogesxxxxx@yahoo.com:451a40fb63d53411f86f4f49b21cc468b058c59a4d41f2fe2
yixxxxxx@upei.ca:614a858c8643cf7e307fd634364f7d6c235f96837c49d0bd4
yinguxxxxx@ou.edu:e85962e3ee35e3f90fb356485c8ebe5b9ec042bac77f1c190
ygxxxxxx@gmail.com:80674b810fc53e53e048f6aacc3c055ddeb349998b9fc5b1a
yemioyxxxxx@yahoo.com:80a0a943d1f509925c7c5552842b4624c2b8effa0d2ec1791
yanninxxxxx@hotmail.com:c18d74cdda28c86615474636d20e2dc5c0b6f2605d570717a
yanghxxxxx@gmail.com:bd4cccf43e5eeee42ec13879f9b0dfd3c5f519658638f3f90
yahya.xxxxx@gmail.com:e61a87f807ec0e2d3f936a7cec7cb5dca8291060ddd212b4b
bendehbia.xxxxxx@hotmail.fr:65324f3ad8e3e85a51740787cf1d1d4bba5c0b84e130e7c60
write2sxxxxxxxxxx@gmail.com:20404051a1d5e96aa0f3a038bd15ce8854b8bbc9b67c2883c
wmsxxxxx@comcast.net:334780689a0ff89ee1034e909bb0bb0bfb4fd732afd7658cf
wincyxxx@hotmail.com:681505cf1cb3907277a081c34c1b72df800d0279d48804e38
jacktxxxxx@yahoo.com:51d94e5885764f3aec7058ba3f28107bcf49c5e79401c3fd6
whitegxxxxxxx@yahoo.com:79918c71701ab71bae7d700d67fd286d21b2f9c3ec513b7e1
whitegxxxxxxx@gmail.com:bc3950cf307a9bc54f103a7ed5275bf724b485c6f1b406bdd

CIRCL #215347 Analysis Stage 1

- What do we get
  - Email addresses : encrypted passwords
  - Bingo: Target site is quoted

Review the site:



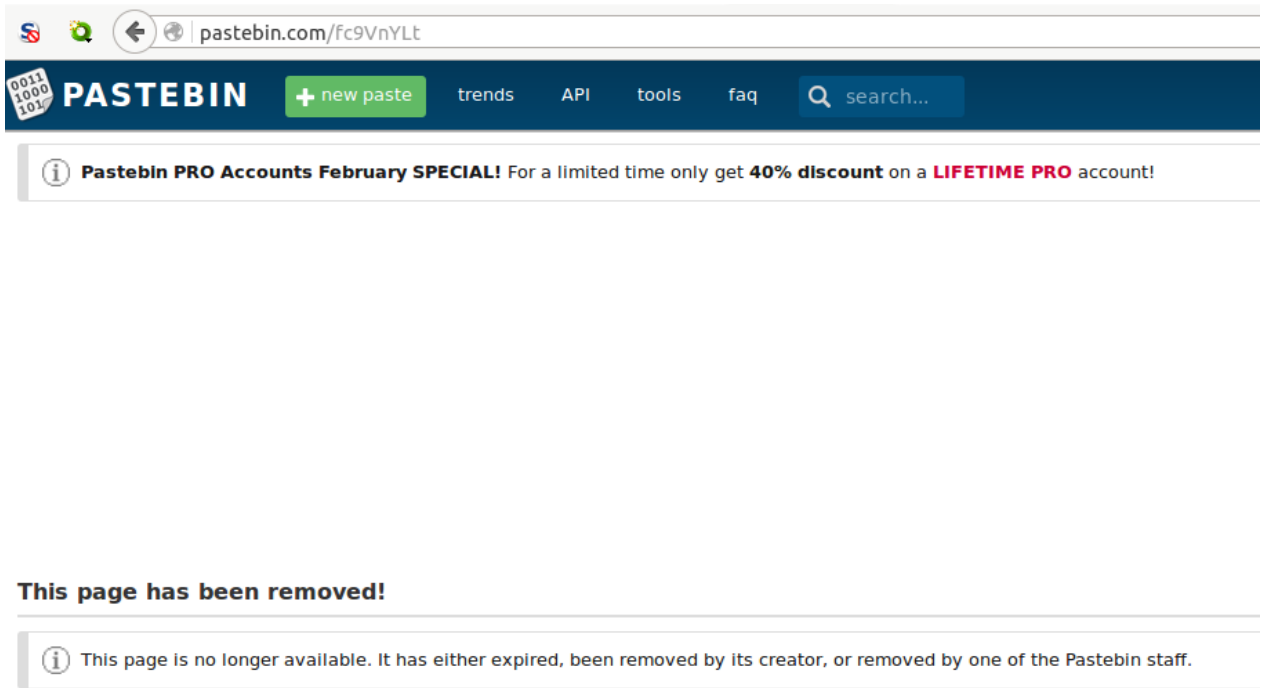
CIRCL #215424 The posting

SEC_EMAIL_ADDRESS.csv
EMAIL_ADDRESS,ENCRYPT_PWD,FIRSTNAME
kente@prairiexxxxxxxx.us,74364AD466A3A97E4D1F7E90490FAE13,Kent
diann@westxxxxxxxx.com,354FA3FB52AAEDAE860431979286EDF0,Diann
klpetxxx@mixxxxxxxx.edu,67357C6CDE1E652C250A75D3764208D8,Kevin
jjamxx@dxxxxx.com,B8AAFA55304D218D9EB11FEE6ADED315,Jim
xxxxhambrick@exxxxxx.com,788F54A6D2CA11FA21A3DEE3F85D3BC9,Jim
xxnope@chxxxxx.net,558EFB24130D85DA042B45CFD2EA94A8,Judith
margexxxxxxxk@txx.com,AFBF5EEDB77DE36B8B559F5F896CDEB6,Marge
ganderxxx@dataxxxxxxx.com,9D9D1E968BC9BA76E5F8D8E8AE4B9CCA,Gisela
bexx@primaryxxxxxxxx.com,22FF6D707D7319F1A0AF8543503D5BC5,Albert
moniquexxxxxxx@ixxx.com,48ABE46CC4C64E840061EC8F65C0AFDD,Monique
deedeexxxxxxxx@cxxxxxxxxxsparks.com,D2AEB85EA85A812D06B849F787074587,Dee dee
xxxlmer@deyoxxxxxx.com,3C7AB6E445E176DD48D4B954FAB1FB31,Johanna
xxxxxxxxxxwilson@hotmail.com,359FCF260D068B42AE7CED3B8C91FD7C,Heather
mhamxxxx@xxxxview.org,A1926ADE8BAE523F9A0990613992065E,Mark
rebecca.xxxxxxxxxx@xx.org,6E1DCB3D49E345DAF44A418E7515480B,Rebecca
marshallxxxxxxx@vxxx.com,E6CE602050FEF4B62AEBD637CE356B47,Marshall
awaxxxxx@hotmail.com,6590B4DC32FE183748680EC7E75D5FE3,Andrew

...//

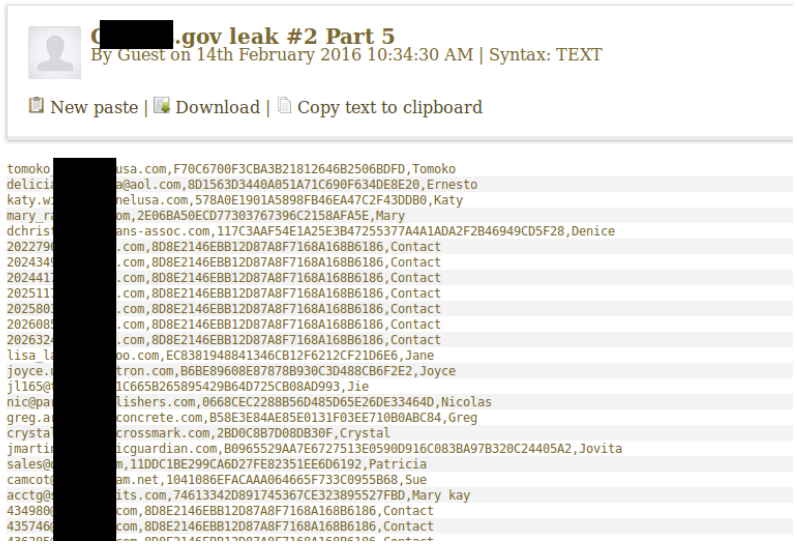
CIRCL #215424 Analysis Stage 1

- Review the posting to gather aditional information
- Unfortunatly already suspended

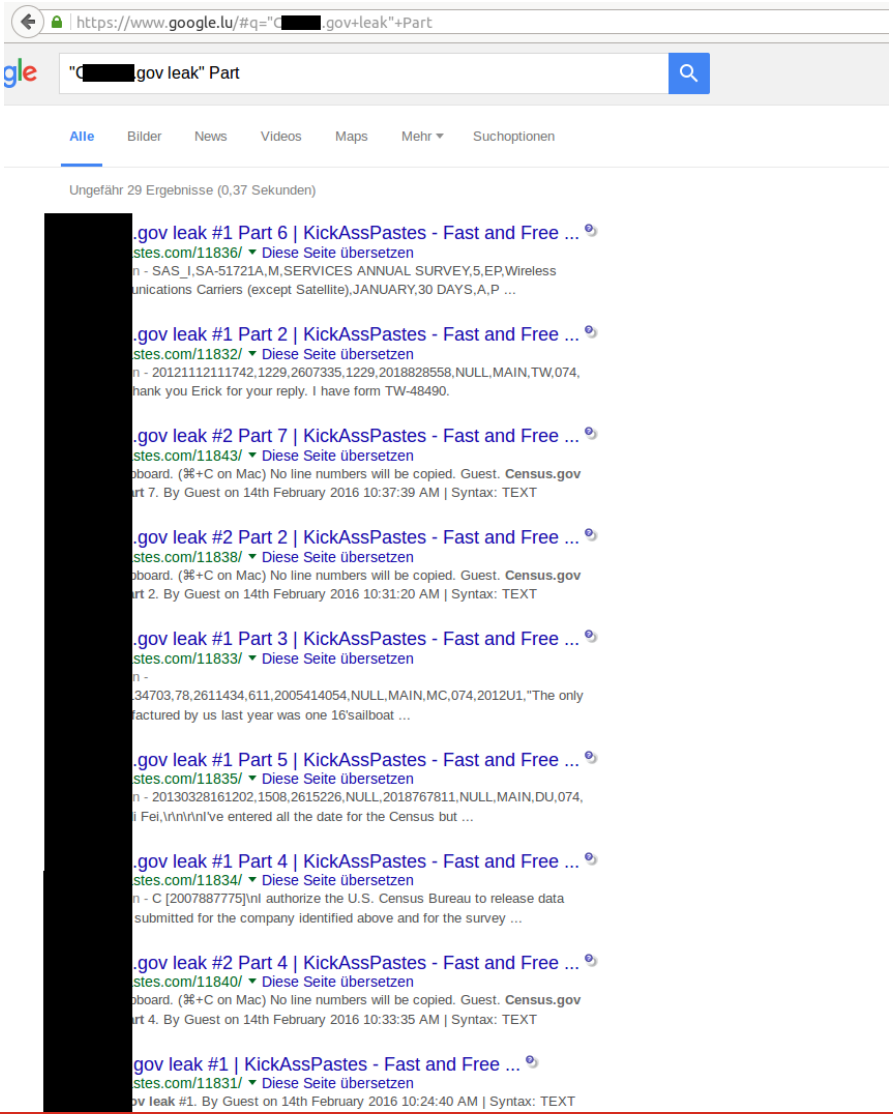


CIRCL #215424 Analysis Stage 1

- Ask Google
- Leads to 1 hit at kickasspastes.com



CIRCL #215424 Search for "*****s.gov leak"



CIRCL #215424 Analyze the set

`wc -l fc9VnYLt.txt`

- 7103

`grep -i "\.mil\," fc9VnYLt.txt`

- 1

`grep -i "\.gov\," fc9VnYLt.txt`

- 175

`grep -i "\.gov\," fc9VnYLt.txt |cut -f1 -d"," |cut -f2 -d"@" |sort |uniq -c |sort -n`

- 1 ******hs.gov
- 1 *****a.gov
- 3 ***.gov
- 170 *****s.gov

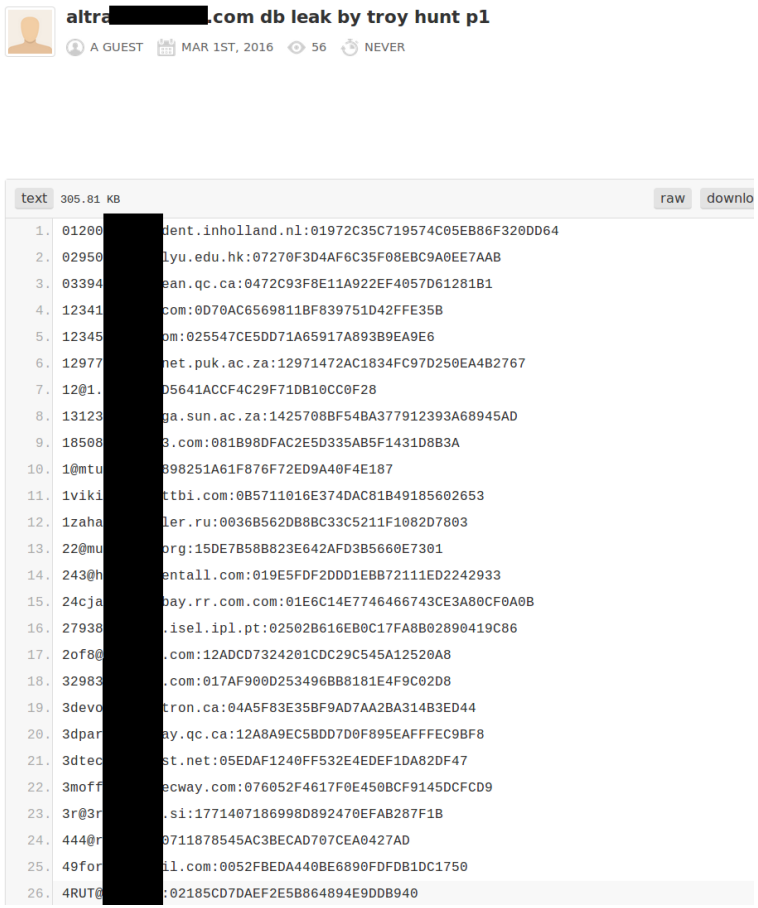
CIRCL #219989 Posting already suspended

```
wc -l BvMacKhC.txt
  ->5728
grep -i "\.mil\:" BvMacKhC.txt
  ->34
grep -i "\.gov\:" BvMacKhC.txt
  ->43
```

Google search for one of the leaked MD5 value

->Leads to 1 hit in Google Cache

CIRCL #219989 From Google cache"



altra[redacted].com db leak by troy hunt p1

A GUEST MAR 1ST, 2016 56 NEVER

text 305.81 KB raw downlo

```
1. 01200[redacted]dent.inholland.nl:01972C35C719574C05EB86F320DD64
2. 02950[redacted]lyu.edu.hk:07270F3D4AF6C35F08EBC9A0EE7AAB
3. 03394[redacted]ean.qc.ca:0472C93F8E11A922EF4057D61281B1
4. 12341[redacted]com:0D70AC6569811BF839751D42FFE35B
5. 12345[redacted]om:025547CE5DD71A65917A893B9EA9E6
6. 12977[redacted]net.puk.ac.za:12971472AC1834FC97D250EA4B2767
7. 12@1.[redacted]D5641ACCF4C29F71DB10CC0F28
8. 13123[redacted]ga.sun.ac.za:1425708BF54BA377912393A68945AD
9. 18508[redacted]3.com:081B98DFAC2E5D335AB5F1431D8B3A
10. 1@mtu[redacted]898251A61F876F72ED9A40F4E187
11. 1viki[redacted]ttbi.com:0B5711016E374DAC81B49185602653
12. 1zaha[redacted]ler.ru:0036B562DB8BC33C5211F1082D7803
13. 22@mu[redacted]org:15DE7B58B823E642AFD3B5660E7301
14. 243@h[redacted]entall.com:019E5FDF2DDD1EBB72111ED2242933
15. 24cja[redacted]bay.rr.com.com:01E6C14E7746466743CE3A80CF0A0B
16. 27938[redacted].isel.ipl.pt:02502B616EB0C17FA8B02890419C86
17. 2of8@[redacted].com:12ADCD7324201CDC29C545A12520A8
18. 32983[redacted].com:017AF900D253496BB8181E4F9C02D8
19. 3devo[redacted]tron.ca:04A5F83E35BF9AD7AA2BA314B3ED44
20. 3dpar[redacted]ay.qc.ca:12A8A9EC5BDD7D0F895EAFFFEC9BF8
21. 3dtec[redacted]st.net:05EDAF1240FF532E4EDEF1DA82DF47
22. 3moff[redacted]ecway.com:076052F4617F0E450BCF9145DCFCD9
23. 3r@3r[redacted].si:1771407186998D892470EFAB287F1B
24. 444@r[redacted]9711878545AC3BECAD707CEA0427AD
25. 49for[redacted]il.com:0052FBEDA440BE6890FDFDB1DC1750
26. 4RUT@[redacted]:02185CD7DAEF2E5B864894E9DDB940
```

CIRCL #219989 Validate the finding

```
grep -i altrx BvMacKhC.txt
```

angela.xxxxxxx@altrxxxxxxx.com:10D56F79CD9DA6496A8627455006FF
chris.xxxx@altrxxxxxxx.com:01E16299BC2ADD4679111FCF0E13A8
dan.xxxxxx@altrxxxxxxx.com:19104E6A08A4DD4C579CFCD8AB7249
dimitrios.xxxxxxxx@altrxxxxxxx:00A4AB56F3F68987E34360DE4B8498

```
whois altryyyyyyyyyyy.com
```

Registrant Organization: Altrx Indxxxxxxx xxxxxx
...

```
whois altrxxxxxxx.com
```

Admin Organization: Altrx Indxxxxxxx xxxxxx
...

CIRCL #215558 pastebin.com/hbjc03Yw

- Grep for ".mil\:"
  - ryan.xxxxxx@xxxxxxxxx.af.mil:chronic
  - Patrick.xxxxxx@xxxxxxxxxxx.af.mil:patrick
  - 48fwxxx@xxxxxxxxxx.af.mil:chapel
  - phillip.xxxxx@xxxxxxxxx.af.mil:allen
- Grep for ".gov\:"
  - kerrixxxx@xxxx.xxi.gov:kerri
- Grep for ".gov"
  1. Leads to 98 hits mainly gov.uk
  2. 1x .gov.ie
  3. 1x .gov.za

CIRCL #215558 Password Frequency Analysis

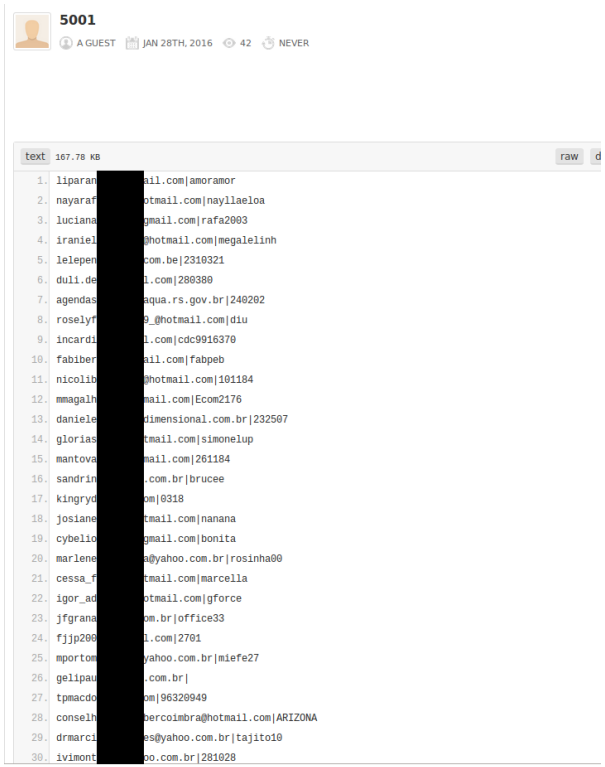
...
...
20 password
22 arsenal
22 daniel
24 george
26 joshua
29 charlie
30 matthew
38 123456
43 111
43 liverpool
121 snooker

CIRCL #215558 Analysis Stage 2

- What do we know
  - Related: co.uk
  - Related: Snooker
- How to find targeted site?

  Google search for: "site:co.uk snooker login"
  –>Unfortunately no helpful results
- What can we do
  1. Go back to the data set
  2. Grep for "snooker"
     –>BINGO

CIRCL #210401 The posting



5001

A GUEST JAN 28TH, 2016 42 NEVER

text 167.78 KB raw d

```
1. liparan[redacted]ail.com|amoramor
2. nayaraf[redacted]otmail.com|nayllaeloa
3. luciana[redacted]gmail.com|rafa2003
4. iraniel[redacted]@hotmail.com|megalelinh
5. lelepen[redacted]com.be|2310321
6. duli.de[redacted]l.com|280380
7. agendas[redacted]aqua.rs.gov.br|240202
8. roselyf[redacted]9_@hotmail.com|diu
9. incardi[redacted]l.com|cdc9916370
10. fabiber[redacted]ail.com|fabpeb
11. nicolib[redacted]@hotmail.com|101184
12. mmagalh[redacted]mail.com|Ecom2176
13. daniele[redacted]dimensional.com.br|232507
14. glorias[redacted]tmail.com|simonelup
15. mantova[redacted]mail.com|261184
16. sandrin[redacted].com.br|brucee
17. kingryd[redacted]om|0318
18. josiane[redacted]tmail.com|nanana
19. cybelio[redacted]gmail.com|bonita
20. marlene[redacted]a@yahoo.com.br|rosinha00
21. cessa_f[redacted]tmail.com|marcella
22. igor_ad[redacted]otmail.com|gforce
23. jfgrana[redacted]om.br|office33
24. fjjp200[redacted]l.com|2701
25. mportom[redacted]yahoo.com.br|miefe27
26. gelipau[redacted].com.br|
27. tpmacdo[redacted]om|96320949
28. conselh[redacted]bercoimbra@hotmail.com|ARIZONA
29. drmarci[redacted]es@yahoo.com.br|tajito10
30. ivimont[redacted]oo.com.br|281028
```

CIRCL #210401 Analysis Stage 1

- What do we got
  - Date
  - Email addresses |passwords
  - –> Leaked 3rd party credentials
  - Obviously many .BR accounts
- What do we miss
  - Usefull information in the header
  - Target details in the posting
- What can we do
  1. Search for interesting accounts
  2. Identify targeted site
  3. Notify our partners in BR

CIRCL #210401 Analysis Stage 2

Search for interesting accounts

graziani.xxxx@xxxx.mar.mil.br—Aprovada

agendaxxxxx@xxxxxxx.rs.gov.br—240202
CLAUDIAxxxxxx@xxxxx.GOV.BR—9395
hellenxxxxxx@xxxxxxx.se.gov.br—33917841
Ocea@xxxxxxxxx.gov.br—180283
escolaxxxxxx@xxxxxxxx.mg.gov.br—171151
nelxxx@xxxxxx.gov.br—np201356
maicxxx@xxxx.rs.gov.br—061188
...
...
26 gov.br users

CIRCL #210401 Analysis Stage 3

Find target: By analyzing the leaked Passwords?

```
cut -f2 -d"|" qzQF6ib5.txt |sort |uniq -c |sort -n
```

```
   4 010203
   4 12345678
   4 hospital
   5 123456789
   6 12345
   6 gabriel
   7 medicina
   8 123
   8 compras
   8 telediu
  13 1234
  79 123456
```

CIRCL #210401 Analysis Stage 3

Find target: By analyzing the leaked Passwords?

`cut grep -i teledi qzQF6ib5.txt`

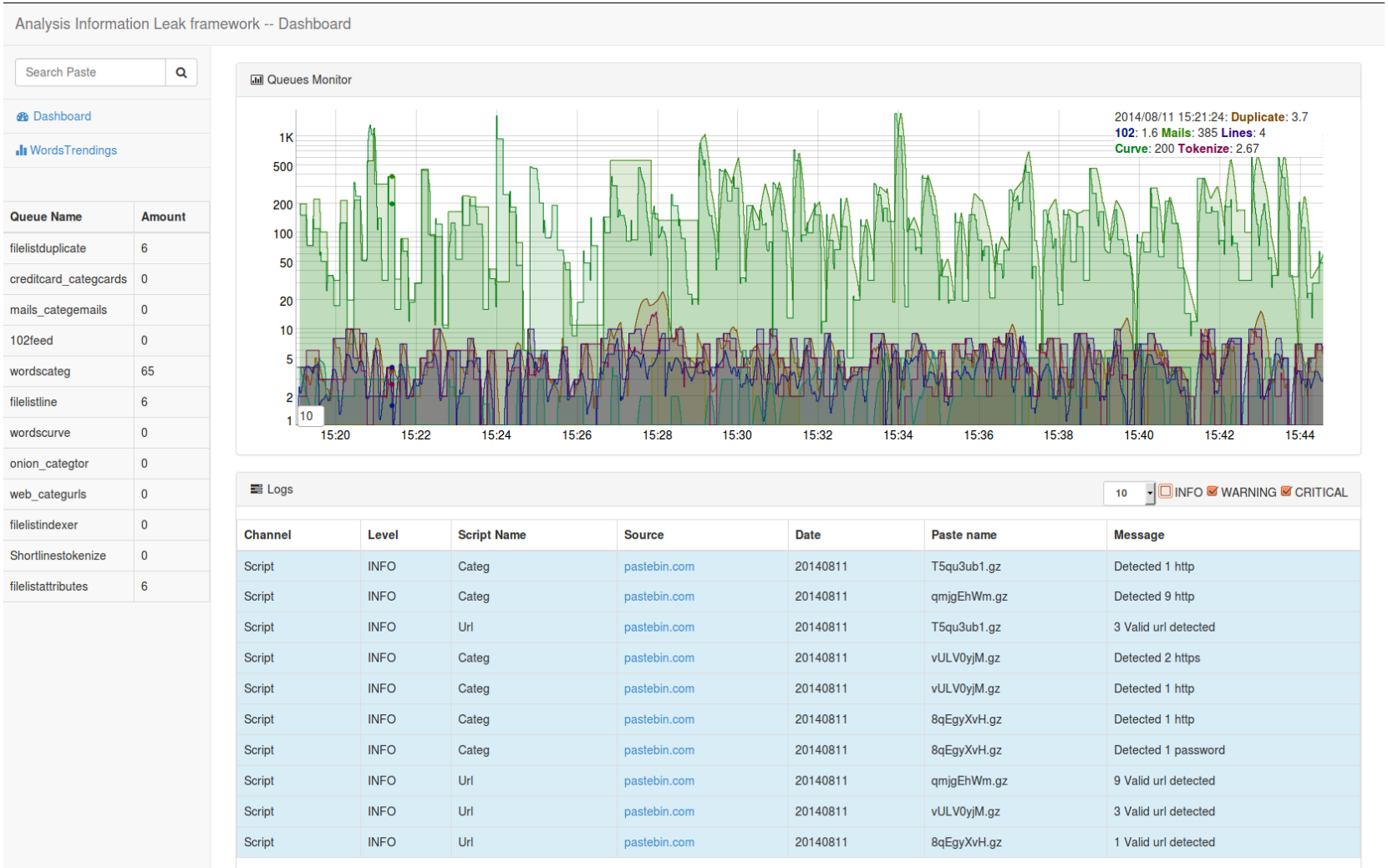
...
8x telediu
...
vanessxxxxxxx@gmail.com—Telediu84
cluciaxxxxxxx@hotmail.com—teledil
tarsisxxxxxxx@hotmail.com—telediu71
amarilxxxxxxx@gmail.com—rodtelediu
heldexxxxxxxx@yahoo.com.br—telediu11
andrexxxxxxxx@yahoo.com.br—telediu150

dentxxxxxxx@telexxxxxxxxxx—233748p
thainapegxxxxxxx@telexxxxxxx—74697649

AIL

- Monitoring Module: Input feeds
- Analysis Module: Deduplication, Indexing, Classification
- Output Module: ZMQ, Redis

AIL


Analysis Information Leak framework -- Dashboard
Search Paste
Dashboard
WordsTrendings
Queue Name
Amount
filelistduplicate 6
creditcard_categcards 0
mails_categemails 0
102feed 0
wordscateg 65
filelistline 6
wordscurve 0
onion_categtor 0
web_categurls 0
filelistindexer 0
Shortlinestokenize 0
filelistattributes 6
Queues Monitor
2014/08/11 15:21:24: Duplicate: 3.7
102: 1.6 Mails: 385 Lines: 4
Curve: 200 Tokenize: 2.67
1K
500
200
100
50
20
10
5
2
1
10
15:20
15:22
15:24
15:26
15:28
15:30
15:32
15:34
15:36
15:38
15:40
15:42
15:44
Logs
10
INFO WARNING CRITICAL
Channel
Level
Script Name
Source
Date
Paste name
Message
Script INFO Categ pastebin.com 20140811 T5qu3ub1.gz Detected 1 http
Script INFO Categ pastebin.com 20140811 qmjgEhWm.gz Detected 9 http
Script INFO Url pastebin.com 20140811 T5qu3ub1.gz 3 Valid url detected
Script INFO Categ pastebin.com 20140811 vULV0yjM.gz Detected 2 https
Script INFO Categ pastebin.com 20140811 vULV0yjM.gz Detected 1 http
Script INFO Categ pastebin.com 20140811 8qEgyXvH.gz Detected 1 http
Script INFO Categ pastebin.com 20140811 8qEgyXvH.gz Detected 1 password
Script INFO Url pastebin.com 20140811 qmjgEhWm.gz 9 Valid url detected
Script INFO Url pastebin.com 20140811 vULV0yjM.gz 3 Valid url detected
Script INFO Url pastebin.com 20140811 8qEgyXvH.gz 1 Valid url detected

Conclusion

- There are no small incidents
- Want access to services: info@circl.lu
- –>search for past issues?